Kentucky Information Technology Standards (KITS)

Full KITS Report - Word Search

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4025	Extensible Markup Language	Extensible Markup Language (XML) is an open standard for describing data from the World Wide Web Consortium (W3C) – a meta-language. XML is a simplified version of Standard Generalized Markup Language (SGML). It is used for defining data elements on a Web page and business-to-business documents. It uses a similar tag structure as HTML; however, whereas HTML defines how elements are displayed, XML defines what those elements contain. HTML uses predefined tags, but XML allows tags to be defined by the developer. There are four principle components that enable XML applications to process an XML document: the XML Document, Document Type Definitions (DTD) or Schemas, Processors and Parsers, and Style Sheets. XML provides a mechanism to label sets of data that can be shared between other systems. The importance of this feature is realized when sharing data between two systems that are operating with different software XML offers state agencies many potential benefits: provide for self-described transactions; enhance workflow and document management functions; interface with legacy systems; reiterate the use of object-based documents and support the implementation of e-government initiatives that must pass data. Approved Standard(s): - XML version 1.0 standard from the World Wide Web Consortium (W3C) - Legal XML standard	A03.040.014	Interface > Application Interface > XML	Extensible Markup Language (XML) defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is defined in the XML 1.0 Specification produced by the World Wide Web Consortium (W3C), and several other related specifications, all gratis open standards.		**Effective:** 5/10/2000 **Revised:** 11/10/2000 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4030	Geographical Information Systems – Shapefile	The ESRI Shapefile is a popular geospatial vector data format for geographic information systems software. An ESRI shapefile consists of a main file, an index file, and a dBASE table. The main file is a direct access, variable-record-length file in which each record describes a shape with a list of its vertices. In the index file, each record contains the offset of the corresponding main file record from the beginning of the main file. The dBASE table contains feature attributes with one record per feature. The one-to-one relationship between geometry and attributes is based on record number. Attribute records in the dBASE file must be in the same order as records in the main file. Approved Standard(s): • Spatial Data Transfer Standard (SDTS), known FIPS 173 for exchange of data created by GIS - Federal Geographic Data Committee (FGDC) Metadata Standard, Sections 1 and 7	A02.024.380	Application Components > Geospatial Information > Cartography	Software that supports the creation of maps.	The ArcGIS suite of products which includes Desktop GIS, Server GIS and Mobile GIS and Online GIS components. Windows 7 Professional 64-bit is the recommended desktop platform as identified in the Kentucky Information Technology Standards Category for Geographic Information Systems (GIS) - Desktop.	**Effective:** 7/1/1997 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4035	Geographical Information Systems – Geodatabases	The geodatabase is a data storage format that is utilized within the ArcGIS suite of software. There are two primary types of geodatabases: file-based and multi-user (enterprise). A file-based geodatabase is stored as binary in a GDB directory structure and can be created using any of the ArcGIS products: ArcView, ArcEditor or ArcGIS Advanced. A multi-user geodatabase is stored in a more powerful relational database management system (RDBMS) like Oracle, Informix, SQL Server or DB2 and must be interfaced with ArcSDE software. Data from a multi-user geodatabase can be read using any of the ArcGIS products, but can only be edited using ArcEditor or ArcGIS Advanced.	A02.024.380	Application Components > Geospatial Information > Cartography	Software that supports the creation of maps.	ArcGIS suite of products - ArcView, ArcEditor or ArcGIS Advanced. ArcSDE.	**Effective:** 7/1/1997 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4050	Recordkeeping - General	A public record is recorded information made or received in conjunction with official agency business that is kept as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government. Statutory definition: “Public record or record" means all books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings, and other documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency. (KRS 171.410, PDF) Approved Standard(s): • Department of Defense (DoD) standard 5015.2 defines baseline records management requirements for electronic systems, based on operational, legislative and legal needs of Federal agencies. This standard has been endorsed by the National Archives and Records Administration. • Records schedules approved by the State Archives and Records Commission reflect known operational, legal, audit, and historical recordkeeping requirements. Agencies must maintain up-to-date and accurate schedules and create and manage records within their framework, in order to fulfill this standard. • Kentucky IT Standards for Electronic Documents – Final Version for Distribution and High Volume Scanners – Digital Imaging specify use of PDF and CCITT III and IV file formats, for non-alterable electronic documents and image files respectively. Other recommended or de facto standard file formats are described in the Kentucky Department for Libraries and Archives’ online publication, Electronic Records Management Guidelines - File Formats	B10.804.345	General Government > General property and records management > Management of Government Records	Management of Government Records involves the management and stewardship of a type of information by the government in order to facilitate communication and information archival. This classification and taxonomic processes that links logical data and information sets.	Products must be listed in DoD 5015.2 plus the supporting technology also must be listed within the Kentucky Information Technology Standards or a KITS Exception is required.	**Effective:** 7/1/1997 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4055	Preservation of Long-term Records	The Preservation of Long-term Records Table represents the digital formats that KDLA has recognized and is encouraging agencies to use when transferring records to the archives. These formats may also be used by agencies when maintaining records with long-term retention (retention period of more than 20 years) in-house. The formats, and corresponding confidence levels, represent KDLA's preferences for long-term preservation. Agencies are free to use other formats (including those not listed) for active business use as long as they meet with state approved standards and architecture. However, systems employed by agencies should support these formats or be able to export records to these formats. The risk level levels identified in the table below are ranked from low (most conducive for long-term preservation) to high (least conducive for long-term preservation.) The risk levels are determined by a combination of sustainability factors including: 1. Documentation. Degree to which complete specifications and tools for validating technical integrity exist and are accessible to those creating and sustaining digital content. Non-proprietary, open standards are usually more fully documented and more likely to be supported by tools for validation than proprietary formats. However, what is most significant for this sustainability factor is not approval by a recognized standards body, but the existence of complete documentation, preferably subject to external expert evaluation. 2. Adoption. Degree to which the format is already used by the primary creators, disseminators, or users of information resources. This includes use as a master format, for delivery to	B10.804.345	General Government > General property and records management > Management of Government Records	Management of Government Records involves the management and stewardship of a type of information by the government in order to facilitate communication and information archival. This classification and taxonomic processes that links logical data and information sets.		**Effective:** 5/19/2010 **Revised:** **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4055		end users, and as a means of interchange between systems. If a format is widely adopted, it is less likely to become obsolete rapidly, and tools for migration and emulation are more likely to emerge. 3. Compression. Many digital formats used for disseminating content employ compression. However, for practical reasons, some digital audio, images, and video may never be stored in an uncompressed form, even when created. Content should be compressed using publicly disclosed and widely adopted algorithms that are either lossless or have a degree of loss compression that is acceptable to the creator, publisher, or primary user as a master version. 4. External Dependencies. Degree to which a particular format depends on particular hardware, operating system, or software for rendering or use and the predicted complexity of dealing with those dependencies in future technical environments. 5. Technical Protection Mechanisms. To preserve digital content and provide service to users and designated communities decades hence, KDLA must be able to replicate the content on new media, migrate and normalize it in the face of changing technology, and disseminate it to users at a resolution consistent with network bandwidth constraints. Content for which KDLA takes long-term responsibility must not be protected by technical mechanisms such as encryption, implemented in ways that prevent custodians from taking appropriate steps to preserve the digital content and make it accessible to future generations. These controls may be necessary for business reasons while the data is in active use in the agency but should be removed upon transfer to the archive.					

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4055		The low and medium risk levels represent the formats that KDLA feels are the most sustainable over time. Agencies should avoid using formats listed in high risk column, or make sure that the records in question can be converted to the formats in the Medium and/or Low risk columns. View the Preservation of Long-term Records Table.					

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4060	Recordkeeping – Electronic Mail	Electronic mail (email) messages are any communication supported by email systems for the conduct of official agency business internally, between other state, local, and federal agencies, and with constituents, voters, vendors, clients, citizens, and others. This definition applies equally to the contents of the communication, the transactional information associated with each message, and any attachments to the body of the message. The email environment in Kentucky state government has a current transaction volume that exceeds eighty million messages a month. This figure dramatically illustrates the extent of agency use and reliance on email services to conduct state business. Two existing Enterprise policies, (1) Status of Electronic Mail as a Public Record, and (2) Internet and Electronic Mail Acceptable Use Policy, CIO-060, have emphasized that electronic mail is statutorily defined as a public record and set broad parameters for the management and acceptable use of email in the executive branch of state government. This standard clarifies agency responsibilities. Approved Standard(s): • KRS sections 061.870 (Open Records) and 171.410 (State Archives and Records) define “public record” to mean all books, papers, maps, photographs, cards, tapes, disks, diskettes, records, and other documentation / documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of, or retained by a public agency. Being public record under these terms, electronic mail must be managed to provide appropriate, reliable, and cost-effective evidence of the business	B10.804.345	General Government > General property and records management > Management of Government Records	Management of Government Records involves the management and stewardship of a type of information by the government in order to facilitate communication and information archival. This classification and taxonomic processes that links logical data and information sets.	See standard for Electronic Mail, Messaging and Collaboration	**Effective:** 3/8/2001 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4060		activities it supports, relates to, or documents. Its integrity, completeness, retrievability, public accessibility, and retention all should respond to agency or Enterprise business requirements. • Agencies establish recordkeeping rules* that are appropriate to the business functions they normally perform. These rules reflect best recordkeeping practices associated with the specific business processes agencies are engaged in, as well as any explicit legal, audit, or archival requirements that have been established. Agencies must apply these recordkeeping rules to the administration of electronic mail as it relates to the same business functions. *The Kentucky Department for Libraries and Archives and the State Archives and Records Commission have statutory authority to establish records management requirements for public agencies of the Commonwealth, and agency recordkeeping practice should conform to standards, schedules, or guidelines developed by them. The following general requirements must be met by agencies in managing email: • The integrity, reliability, and authenticity of email messages must be protected through compliance with all security and data management requirements established in the Enterprise Architecture and Standards. • Per the acceptable use policy referenced above, agencies must instruct employees and take steps to ensure that non-business related email messages are regularly deleted from email stores (inboxes and personal folders). Transitory messages, which are defined as messages that are for informational and reference purposes only and do not set policy, establish guidelines or procedures, certify a					

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4060		transaction, or become a receipt, must also be routinely disposed of. • Retention periods for email messages vary according to the functions they are associated with. It is the responsibility of the agency to codify retention practices through development of records schedules in cooperation with the Kentucky Department for Libraries and Archives. Retention requirements cannot be met through routine agency backups, and agency staff must be made fully aware of this and the appropriate schedules that must be created and adhered to. • EAS Appendix G, Guidelines for Managing E-Mail in Kentucky State Government, promulgated by the Department for Libraries and Archives, provides agencies with further guidance on the implementation of this standard.					

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4065	Data Governance – Data Stewardship	The fundamental building block of the Enterprise Architecture and Standards is data – it is a critical state resource and must be managed as such. Data must be thought of as a strategic enterprise resource and not as belonging exclusively to one program, agency or individual. A statewide shift in mindset must be made away from local data ownership and towards local data stewardship. A steward is an individual who manages something on behalf of someone else. Accordingly, the role of a Data Steward is to manage the data of an agency functional/program area on behalf of the Commonwealth at large. To assure that maximum benefit is derived from the sharing, integration and utilization of data for both program-level tactical applications and multi-agency strategic predictive planning, decisions regarding data must also be made at the enterprise level. The Division of Enterprise Architecture and the Information Technology Standards Committee (ITSC) are the appropriate venues for those decisions to be made. Approved Standard(s): Executive branch agencies are responsible for assigning data stewardship responsibilities to designated staff, to facilitate the proper management of data as a strategic resource for the enterprise. This responsibility is assumed to encompass the standardization and appropriate sharing and integration of data resources, consistent with state and Federal laws and the vision of the Kentucky Enterprise Data Architecture.	B10.811.KY001	General Government > Information sharing > Data Governance	Refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise.	IBM InfoSphere Information Governance Catalog IBM Glossary Anywhere	**Effective:** 1/1/2008 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4070	Common Data Definitions	A core set of common data definitions, formats, type, and size and code values for enterprise data elements. A unique identifier for both individuals and organizations that associates data to a single entity is a critical element of the data definition. Approved Standard(s): • The Enterprise Common Data Definitions related to individual and organizational identity only, are fully described in the documentation on the Enterprise Common Data Model Framework. • The enterprise policy directing the use of Enterprise Common Data Definitions by state agencies and incorporating the recommendations into the Enterprise Standards by reference: Commonwealth Office of Technology Policy Directive – “Policy Statement Relating to Enterprise Data Standards” (adopted Dec 13, 2007). See https://gotsource.ky.gov/docushare/dsweb/Get/Document-115912/	B10.811.604	General Government > Information sharing > Meta Data Management	Support the maintenance and administration of data that describes data.	IBM InfoSphere Information Governance Catalog IBM Glossary Anywhere CA - ERwin IBM InfoSphere Data Architect	**Effective:** 1/1/2008 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4080	Data Classification Standard	This standard establishes the criteria for classifying data and information into three categories: Non-Sensitive, Sensitive and Confidential. This classification matrix in no way supersedes the Open Records Act requirements of State Government (KRS 61.870 to 61.884). Classification is important because it determines the level of security to be applied to the data, any application that processes the data, and the environment which houses/stores the data. As would be expected, sensitive and confidential data require more stringent security while non-sensitive requires very little security (only controls over the integrity and availability of the data may be necessary). All Commonwealth data must be appropriately reviewed to determine its classification. This classification will be used for, but is not limited to, determining limitations on the use, protection and storage of the data. If data is interdependent with other data that is classified with a higher level of sensitivity, the classification that requires the most stringent controls should be used.	S01.001.001	Purpose > Regulatory Conditions > Executive Branch Directives	Executive Orders, Memoranda, security directives regarding classification and protection of federal information or other security goals. See FIPS 200, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-37, and CNSSI-4009.		**Effective:** 9/16/2009 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4090	Data Integration	Data integration is the process of combining data residing at different sources to provide a unified view of these data. Data integration can be classified in four different types of integration based on the characteristics of the data movement. • Enterprise Application Integration (EAI) – Usually associated with use between two existing systems where at least one is a transaction processing system. Characteristics of EAI: Transaction based data ; Data is usually structured (file layouts) ; Messaging transport is used (MSMQ, MQ, File, etc) ; Low transformation of the data ; Translation of data is usually performed ; Usually associated with Process Integration ; Commonly event driven and/or real time processing. Common architectures: Web Services (Point to Point)/Service Interface (IMS/CICS) ; IBM MQ/MSMQ ; ESB (IBM Message Broker, MS BizTalk) ; Remote Procedure Call (RPC) • Extract-Transform-Load (ETL) – Used to communicate between two or more systems where the systems can be a transaction processing system, management information system or decision support system. Characteristics of ETL: Record based data ; Usually derived data ; High volume ; Movement of data from store to store ; Structured or Semi-structured data ; Usually associated with Process Integration ; Batch based (right time) Common architectures: ETL Tools (SAS, IBM DataStage/QualityStage) ; Custom extract programs (batch) ; Ad-Hoc query tools Microsoft Excel, etc) • Data Replication – Used to copy data from one data store to another for duplication of data from one system to another. Characteristics of Data Replication:	B10.811.601	General Government > Information sharing > Data Exchange	Supports the interchange of information between multiple systems and applications; includes verification that transmitted data was received unaltered.	IBM InfoSphere FastTrack IBM InfoSphere DataStage IBM InfoSphere QualityStage IBM InfoSphere Information Services Director IBM InfoSphere Federation Server	**Effective:** 9/16/2009 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4090		Data store to data store copy ; Structured data ; Low transformation of the data ; Used when high availability is necessary ; Usually associated with Analytical Systems Common architectures: Database vendor tools (IBM ReplicationServer) ; Compuware File-Aid (IMS, DB2, etc) ; Third party database tools • Federation – Used to facilitate access to data while leaving the data in place within the source system. Characteristics of Federation: Query based ; Usually multiple data sources ; Structured/Semi-structured data ; Moderate transformation ; Wrappers are utilized to provide consistency of data ; Real time – need the most current data ; Usually associated with Analytical Systems ; Medium to high volume. Common architectures: IBM Classic Federation (z/os data stores – IMS, VSAM, QSAM, etc) ; IBM Federate Server (distributed data stores) View more information related to this standard at https://gotsource.ky.gov/docushare/dsweb/Get/Document-301107/					

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
4350	Electronic Commerce – Electronic Data Interchange (EDI)	Electronic data interchange (EDI) is the secure electronic communication of business transactions, such as purchase orders, confirmations, invoices, and other data between organizations. EDI may be used to submit data to a state agency in a standard, prescribed format, with translation software required to complete the communication. Value added networks (VANs) act as third parties to provide EDI services that enable organizations with different equipment to connect. The EDI format chosen must provide proper security controls to protect the Confidentiality and integrity of the data during transmission. The two approved standards are: ANSI ASC X12 UN/EDIFACT The ANSI ASC X12 EDI standard defines the data structure and content for business transactions transmitted between computer applications. The United Nations Rules for Electronic Data Interchange For Administration, Commerce and Transport (UN/EDIFACT) is a set of internationally agreed upon standards, directories and guidelines for the electronic interchange of structured data that relate, in particular, to trade in goods and services.	B10.811.601	General Government > Information sharing > Data Exchange	Supports the interchange of information between multiple systems and applications; includes verification that transmitted data was received unaltered.		**Effective:** 7/1/1997 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015